PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2005-285089
(43)Date of publication of application : 13.10.2005

(51)Int.Cl. G06F 12/14
H04L 9/32

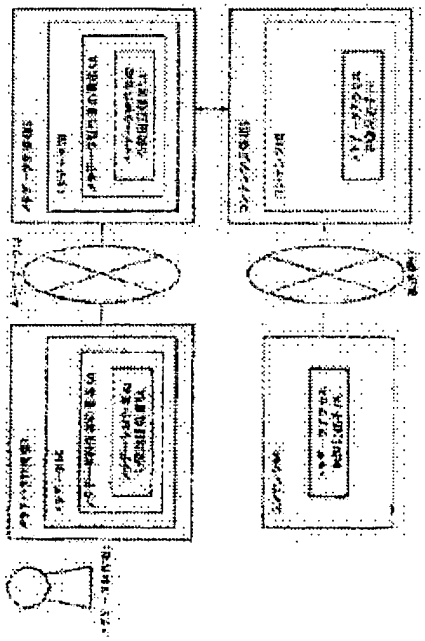
(21)Application number : 2004-358517
(22)Date of filing : 10.12.2004

(71)Applicant : NEC CORP
NIPPON HOSO KYOKAI <NHK>
(72)Inventor : GOTO ATSUSHI
NISHIMOTO TOMONARI
BABA AKITSUGU
NAKAMURA HARUYUKI
ISHIKAWA KIYOHIKO
KURIOKA TATSUYA

(30)Priority
Priority number : 2004060085 Priority date : 04.03.2004 Priority country : JP

(54) ACCESS CONTROL METHOD, ACCESS CONTROL SYSTEM, META DATA CONTROLLER, AND TRANSMISSION SYSTEM DEVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To control an enabled/disabled state of an access from meta data to contents.
SOLUTION: The access control method includes: a step for generating meta data 3A for a content 6A and embedding a digital signature 4A of a creator who has created the meta data as creator information in the created meta data 3A; a step for embedding an identifier 5A indicating from which meta data an access to the contents is allowed, in the license information required for reproducing the contents 6A; and an access enabled/disabled control step for controlling an access enabled/disabled state to the contents 6A from the created meta data 3A by comparing the digital signature 4A with the identifier 5A.



(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2005-285089
(P2005-285089A)
(43)公開日　平成17年10月13日(2005.10.13)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G06F 12/14	G06F 12/14	520C	5B017
H04L 9/32	G06F 12/14	540B	5J104
	H04L 9/00	675B	

審査請求 有　請求項の数 32　OL　（全 22 頁）

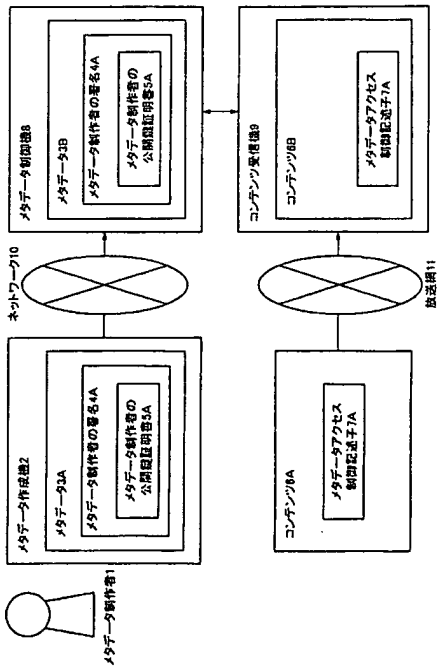
(21)出願番号　特願2004-358517 (P2004-358517)
(22)出願日　平成16年12月10日 (2004.12.10)
(31)優先権主張番号　特願2004-60085 (P2004-60085)
(32)優先日　平成16年3月4日 (2004.3.4)
(33)優先権主張国　日本国(JP)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(71)出願人　000004352
日本放送協会
東京都渋谷区神南２丁目２番１号
(74)代理人　100077838
弁理士　池田　憲保
(72)発明者　後藤　淳
東京都港区芝五丁目７番１号　日本電気株式会社内
(72)発明者　西本　友成
東京都世田谷区砧一丁目１０番１１号　日本放送協会放送技術研究所内

最終頁に続く

(54)【発明の名称】アクセス制御方法、アクセス制御システム、メタデータ制御機、及び送信系装置

(57)【要約】
【課題】メタデータからコンテンツへのアクセスの可・不可を制御するアクセス制御方法の提供。
【解決手段】コンテンツ６Aに対するメタデータ３Aを制作し、制作されたメタデータ３A中に該メタデータを制作した制作者の電子署名４Aを制作者情報として埋め込むステップと、コンテンツ６Aを再生するのに必要なライセンス情報に、どのメタデータからコンテンツへのアクセスを許可するかを示す識別子５Aを予め埋め込んでおくステップと、電子署名４Aと識別子５Aとを突き合わせることで、前記制作されたメタデータ３Aからコンテンツ６Aに対するアクセスの可否を制御するアクセス可否制御ステップとを有することを特徴とするアクセス制御方法。
【選択図】図１



【特許請求の範囲】
【請求項１】
コンテンツに対して制作されたメタデータ中に該メタデータを制作した制作者を示す制作者情報を埋め込む制作者情報埋め込みステップと、
前記コンテンツを再生するのに必要なライセンス情報に、どのメタデータからコンテンツへのアクセスを許可するかを示す識別子を予め埋め込んでおくステップと、
前記制作者情報と前記識別子とを突き合わせることで、前記制作されたメタデータから前記コンテンツに対するアクセスの可否を制御するアクセス可否制御ステップとを有することを特徴とするアクセス制御方法。
【請求項２】
請求項１に記載のアクセス制御方法において、
前記識別子は、前記コンテンツへのアクセスが許可されるメタデータの制作者を示すメタデータアクセス制御記述子であることを特徴とするアクセス制御方法。
【請求項３】
請求項１に記載のアクセス制御方法において、
前記制作者情報埋め込みステップは、コンテンツに対して制作されたメタデータ中に該メタデータを制作した制作者を示す電子署名を、前記制作者情報として、埋め込む電子署名埋め込みステップであり、
前記アクセス可否制御ステップは、前記電子署名と前記識別子とを突き合わせることで、前記制作されたメタデータから前記コンテンツに対するアクセスの可否を制御するステップであることを特徴とするアクセス制御方法。
【請求項４】
請求項３に記載のアクセス制御方法において、
前記識別子は、前記コンテンツへのアクセスが許可されるメタデータの制作者を示すメタデータアクセス制御記述子であることを特徴とするアクセス制御方法。
【請求項５】
請求項３に記載のアクセス制御方法において、
前記電子署名は、公開鍵基盤（ＰＫＩ）技術にもとづき前記制作者としての署名者を特定することができるものであることを特徴とするアクセス制御方法。
【請求項６】
請求項３に記載のアクセス制御方法において、
前記識別子は、前記コンテンツへのアクセスが許可されるメタデータの制作者を示すメタデータアクセス制御記述子であり、
前記電子署名は、前記制作者としての署名者の公開鍵証明書の情報を含み、
前記アクセス可否制御ステップは、前記公開鍵証明書の情報が前記メタデータアクセス制御記述子によって示される制作者として識別される場合に、前記制作されたメタデータから前記コンテンツへのアクセスを許可し、前記制作されたメタデータに基づいて前記コンテンツの映像を見ることを可能としたことを特徴とするアクセス制御方法。
【請求項７】
請求項１に記載のアクセス制御方法において、
前記制作されたメタデータがメタデータ作成機において作成されたメタデータであり、該作成されたメタデータ中に該メタデータを作成した作成者の情報が、前記制作者情報として、埋め込まれることを特徴とするアクセス制御方法。
【請求項８】
請求項１に記載のアクセス制御方法において、
前記制作されたメタデータがメタデータ制御機において追加編集されたメタデータであり、該追加編集されたメタデータ中に該メタデータを追加編集した制作者の情報が、前記制作者情報として、埋め込まれることを特徴とするアクセス制御方法。
【請求項９】
請求項３に記載のアクセス制御方法において、

前記制作されたメタデータがメタデータ作成機において作成されたメタデータであり、該作成されたメタデータ中に該メタデータを作成した作成者の電子署名が、前記制作者情報として、埋め込まれることを特徴とするアクセス制御方法。

【請求項１０】

請求項３に記載のアクセス制御方法において、

前記制作されたメタデータがメタデータ制御機において追加編集されたメタデータであり、該追加編集されたメタデータ中に該メタデータを追加編集した制作者の電子署名が、前記制作者情報として、埋め込まれることを特徴とするアクセス制御方法。

【請求項１１】

コンテンツに対して制作されたメタデータ中に該メタデータを制作した制作者を示す制作者情報を埋め込む制作者情報埋め込み手段と、

前記コンテンツを再生するのに必要なライセンス情報に、どのメタデータからコンテンツへのアクセスを許可するかを示す識別子を予め埋め込んでおく識別子埋め込み手段と、

前記制作者情報と前記識別子とを突き合わせることで、前記制作されたメタデータから前記コンテンツに対するアクセスの可否を制御するアクセス可否制御手段とを有することを特徴とするアクセス制御システム。

【請求項１２】

請求項１１に記載のアクセス制御システムにおいて、

前記識別子は、前記コンテンツへのアクセスが許可されるメタデータの制作者を示すメタデータアクセス制御記述子であることを特徴とするアクセス制御システム。

【請求項１３】

請求項１１に記載のアクセス制御システムにおいて、

前記制作者情報埋め込み手段は、コンテンツに対して制作されたメタデータ中に該メタデータを制作した制作者を示す電子署名を、前記制作者情報として、埋め込む電子署名埋め込み手段であり、

前記アクセス可否制御手段は、前記電子署名と前記識別子とを突き合わせることで、前記制作されたメタデータから前記コンテンツに対するアクセスの可否を制御する手段であることを特徴とするアクセス制御システム。

【請求項１４】

請求項１３に記載のアクセス制御システムにおいて、

前記識別子は、前記コンテンツへのアクセスが許可されるメタデータの制作者を示すメタデータアクセス制御記述子であることを特徴とするアクセス制御システム。

【請求項１５】

請求項１３に記載のアクセス制御システムにおいて、

前記電子署名は、公開鍵基盤（ＰＫＩ）技術にもとづき前記制作者としての署名者を特定することができるものであることを特徴とするアクセス制御システム。

【請求項１６】

請求項１３に記載のアクセス制御システムにおいて、

前記識別子は、前記コンテンツへのアクセスが許可されるメタデータの制作者を示すメタデータアクセス制御記述子であり、

前記電子署名は、前記制作者としての署名者の公開鍵証明書の情報を含み、

前記アクセス可否制御ステップは、前記公開鍵証明書の情報が前記メタデータアクセス制御記述子によって示される制作者として識別される場合に、前記制作されたメタデータから前記コンテンツへのアクセスを許可し、前記制作されたメタデータに基づいて前記コンテンツの映像を見ることを可能としたことを特徴とするアクセス制御システム。

【請求項１７】

請求項１１に記載のアクセス制御システムにおいて、

前記制作されたメタデータがメタデータ作成機において作成されたメタデータであり、該作成されたメタデータ中に該メタデータを作成した作成者の情報が、前記制作者情報として、埋め込まれることを特徴とするアクセス制御システム。

【請求項１８】
請求項１１に記載のアクセス制御システムにおいて、
前記制作されたメタデータがメタデータ制御機において追加編集されたメタデータであり、該追加編集されたメタデータ中に該メタデータを追加編集した制作者の情報が、前記制作者情報として、埋め込まれることを特徴とするアクセス制御システム。
【請求項１９】
請求項１３に記載のアクセス制御システムにおいて、
前記制作されたメタデータがメタデータ作成機において作成されたメタデータであり、該作成されたメタデータ中に該メタデータを作成した作成者の電子署名が、前記制作者情報として、埋め込まれることを特徴とするアクセス制御システム。
【請求項２０】
請求項１３に記載のアクセス制御システムにおいて、
前記制作されたメタデータがメタデータ制御機において追加編集されたメタデータであり、該追加編集されたメタデータ中に該メタデータを追加編集した制作者の電子署名が、前記制作者情報として、埋め込まれることを特徴とするアクセス制御システム。
【請求項２１】
コンテンツを受信し再生する機能を有すると共に、前記コンテンツを再生するのに必要なライセンス情報に埋め込まれた、どのメタデータからコンテンツへのアクセスを許可するかを示す識別子を受信する機能を有するコンテンツ受信部に組合されて使用されるメタデータ制御機において、
前記コンテンツに対して制作されたメタデータと、制作されたメタデータ中に埋め込まれた、該メタデータを制作した制作者を示す制作者情報とを受信する機能と、
前記コンテンツ受信部から前記識別子を取得し、前記メタデータ中の前記制作者情報と前記識別子とを突き合わせることで、前記制作されたメタデータから前記コンテンツ受信部内の前記コンテンツに対するアクセスの可否を制御するアクセス可否制御機能とを有することを特徴とするメタデータ制御機。
【請求項２２】
請求項２１に記載のメタデータ制御機において、
前記識別子は、前記コンテンツへのアクセスが許可されるメタデータの制作者を示すメタデータアクセス制御記述子であることを特徴とするメタデータ制御機。
【請求項２３】
請求項２１に記載のメタデータ制御機において、
前記制作者情報が、前記メタデータを制作した制作者を示す電子署名であることを特徴とするメタデータ制御機。
【請求項２４】
請求項２３に記載のメタデータ制御機において、
前記識別子は、前記コンテンツへのアクセスが許可されるメタデータの制作者を示すメタデータアクセス制御記述子であることを特徴とするメタデータ制御機。
【請求項２５】
請求項２３に記載のメタデータ制御機において、
前記電子署名は、公開鍵基盤（ＰＫＩ）技術にもとづき前記制作者としての署名者を特定することができるものであることを特徴とするメタデータ制御機。
【請求項２６】
請求項２３に記載のメタデータ制御機において、
前記識別子は、前記コンテンツへのアクセスが許可されるメタデータの制作者を示すメタデータアクセス制御記述子であり、
前記電子署名は、前記制作者としての署名者の公開鍵証明書の情報を含み、
前記メタデータ制御機は、前記公開鍵証明書の情報が前記メタデータアクセス制御記述子によって示される制作者として識別される場合に、前記制作されたメタデータから前記コンテンツ受信部内の前記コンテンツへのアクセスを許可し、前記制作されたメタデータ

に基づいて前記コンテンツの映像を見ることを可能としたことを特徴とするメタデータ制御機。

【請求項２７】

コンテンツを受信系装置に送信するコンテンツ送信装置と、前記コンテンツに対して制作されたメタデータを前記受信系装置に送信するメタデータ送信装置とを有する送信系装置において、

前記メタデータ送信装置は、前記制作されたメタデータを、前記制作されたメタデータ中に該メタデータを制作した制作者を示す制作者情報を埋め込んだ状態にて前記受信系装置に送信する機能を有し、

前記コンテンツ送信装置は、前記コンテンツを再生するのに必要なライセンス情報を、該ライセンス情報に、どのメタデータからコンテンツへのアクセスを許可するかを示す識別子を埋め込んだ状態にて前記受信系装置に送信する機能を有し、

前記送信系装置は、前記受信系装置に、前記メタデータ送信装置から受信した前記制作者情報と前記コンテンツ送信装置から受信した前記識別子との突き合わせで、前記制作されたメタデータから前記コンテンツに対するアクセスの可否を制御可能とさせたことを特徴とする送信系装置。

【請求項２８】

請求項２７に記載の送信系装置において、

前記識別子は、前記コンテンツへのアクセスが許可されるメタデータの制作者を示すメタデータアクセス制御記述子であることを特徴とする送信系装置。

【請求項２９】

請求項２７に記載の送信系装置において、

前記制作者情報が、前記メタデータを制作した制作者を示す電子署名であることを特徴とする送信系装置。

【請求項３０】

請求項２９に記載の送信系装置において、

前記識別子は、前記コンテンツへのアクセスが許可されるメタデータの制作者を示すメタデータアクセス制御記述子であることを特徴とする送信系装置。

【請求項３１】

請求項２９に記載の送信系装置において、

前記電子署名は、公開鍵基盤（ＰＫＩ）技術にもとづき前記制作者としての署名者を特定することができるものであることを特徴とする送信系装置。

【請求項３２】

請求項２９に記載の送信系装置において、

前記識別子は、前記コンテンツへのアクセスが許可されるメタデータの制作者を示すメタデータアクセス制御記述子であり、

前記電子署名は、前記制作者としての署名者の公開鍵証明書の情報を含み、

前記送信系装置は、前記受信系装置において、前記公開鍵証明書の情報が前記メタデータアクセス制御記述子によって示される制作者として識別される場合に、前記受信系装置における、前記制作されたメタデータから前記コンテンツへのアクセスを許可し、前記受信系装置に、前記制作されたメタデータに基づいて前記コンテンツの映像を見ることを可能とさせたことを特徴とする送信系装置。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、デジタル放送におけるメタデータからコンテンツへのアクセス制御方法に関するものである。

【背景技術】

【０００２】

サーバー型放送は、受信機に番組蓄積装置と通信接続機能を備えることで、放送時間に

拘束されない番組視聴を実現する。さらに、コンテンツプロバイダーがメタデータと呼ばれる番組関連情報を提供することで、ハイライト的な番組視聴などの多様な放送サービスを実現する。例えば、野球中継番組においてある打者の打撃シーンのみをダイジェストとして視聴するなどのサービスが挙げられる。このサービスは、コンテンツプロバイダーが、当該野球中継番組を示す番組名と前記打者のすべての打撃シーンの開始時間位置を示す情報とを含むメタデータを制作し、当該メタデータを視聴者に提供することにより、実現される。また、魅力あるメタデータを安価に制作するために、コンテンツプロバイダーだけでなく、ネットワークプロバイダーや、第三者機関やユーザなどがメタデータを制作することが想定されている。

【０００３】

一方で、このメタデータを改竄したり、不正なメタデータを制作することで、ＣＭのみを除いた番組視聴や、複数の番組のシーンをつないで別の番組を作成するなど、コンテンツプロバイダーの意向にもとづかない番組利用が行われる恐れがある。そのため、不正なメタデータの氾濫を防止するために、メタデータの改竄を防止し、番組ごとに、利用を許可するメタデータをコンテンツプロバイダーが指定できる必要がある。

【０００４】

非特許文献１には、標準規格ARIB(Association of Radio Industries and Businesses) STD-B38（サーバー型放送における符号化、伝送及び蓄積制御方式）の概要が記載され、特に、サーバー型放送の概念が図示されている。

【０００５】

ARIB STD-B38の規格中には、XML(Extensible Markup Language)形式による番組のメタデータの記述方法が定義されている。ARIB STD-B38の規格では、コンテンツに対する付加情報をメタデータに記述し再生端末に表示するだけでなく、メタデータの記述に基づいたコンテンツの部分再生などの再生制御のための情報を記述できるよう定義されている。メタデータからコンテンツを再生する機能を有する再生機を利用すると、コンテンツの部分再生やコンテンツ自体を編集せずにコンテンツのダイジェスト版を定義・再生することが可能となる。

【０００６】

ここで、メタデータ自体はXMLで記述されるため、誰でも簡単に作成できる。そのため、コンテンツ自体にアクセスできれば誰でも簡単にコンテンツのダイジェスト版が作成できてしまうので、作成者Ａが作成したメタデータからはアクセスを受け付けるが、Ｂが作成したメタデータからはアクセスを受け付けない、というようなコンテンツに対するアクセス制御を実現する必要があった。

【０００７】

【非特許文献１】標準規格概要（放送分野）　規格番号：ARIB STD-B38　標準規格名：サーバー型放送における符号化、伝送及び蓄積制御方式、[online]、社団法人電波産業会、[２００４年１月２９日検索]、インターネット＜URL：http://www.arib.or.jp/tyosakenkyu/kikaku_hoso/hoso_std-b038.html＞

【発明の開示】

【発明が解決しようとする課題】

【０００８】

本発明の目的は、メタデータとコンテンツが配信され、メタデータによってコンテンツの再生制御の機能が実現されるサーバ型放送において、メタデータの制作者によってコンテンツへのアクセスの可・不可を制御するアクセス制御方法を提供することにある。

【０００９】

本発明の別の目的は、上述のアクセス制御方法を実施するアクセス制御システムを提供することにある。

【００１０】

本発明の他の目的は、メタデータの制作者によってコンテンツへのアクセスの可否を制御するメタデータ制御機を提供することにある。

【００１１】
本発明の更に他の目的は、受信系装置に、メタデータの制作者によってコンテンツへのアクセスの可否を制御可能とさせる送信系装置を提供することにある。
【課題を解決するための手段】
【００１２】
本発明によれば、
コンテンツに対して制作されたメタデータ中に該メタデータを制作した制作者を示す制作者情報を埋め込む制作者情報埋め込みステップと、
前記コンテンツを再生するのに必要なライセンス情報に、どのメタデータからコンテンツへのアクセスを許可するかを示す識別子を予め埋め込んでおくステップと、
前記制作者情報と前記識別子とを突き合わせることで、前記制作されたメタデータから前記コンテンツに対するアクセスの可否を制御するアクセス可否制御ステップとを有することを特徴とするアクセス制御方法が得られる。
【００１３】
更に、本発明によれば、
コンテンツに対して制作されたメタデータ中に該メタデータを制作した制作者を示す制作者情報を埋め込む制作者情報埋め込み手段と、
前記コンテンツを再生するのに必要なライセンス情報に、どのメタデータからコンテンツへのアクセスを許可するがを示す識別子を予め埋め込んでおく識別子埋め込み手段と、
前記制作者情報と前記識別子とを突き合わせることで、前記制作されたメタデータから前記コンテンツに対するアクセスの可否を制御するアクセス可否制御手段とを有することを特徴とするアクセス制御システムが得られる。
【００１４】
また、本発明によれば、
コンテンツを受信し再生する機能を有すると共に、前記コンテンツを再生するのに必要なライセンス情報に埋め込まれた、どのメタデータからコンテンツへのアクセスを許可するかを示す識別子を受信する機能を有するコンテンツ受信部に組合されて使用されるメタデータ制御機において、
前記コンテンツに対して制作されたメタデータと、制作されたメタデータ中に埋め込まれた、該メタデータを制作した制作者を示す制作者情報とを受信する機能と、
前記コンテンツ受信部から前記識別子を取得し、前記メタデータ中の前記制作者情報と前記識別子とを突き合わせることで、前記制作されたメタデータから前記コンテンツ受信部内の前記コンテンツに対するアクセスの可否を制御するアクセス可否制御機能とを有することを特徴とするメタデータ制御機が得られる。
【００１５】
更に、本発明によれば、
コンテンツを受信系装置に送信するコンテンツ送信装置と、前記コンテンツに対して制作されたメタデータを前記受信系装置に送信するメタデータ送信装置とを有する送信系装置において、
前記メタデータ送信装置は、前記制作されたメタデータを、前記制作されたメタデータ中に該メタデータを制作した制作者を示す制作者情報を埋め込んだ状態にて前記受信系装置に送信する機能を有し、
前記コンテンツ送信装置は、前記コンテンツを再生するのに必要なライセンス情報を、該ライセンス情報に、どのメタデータからコンテンツへのアクセスを許可するかを示す識別子を埋め込んだ状態にて前記受信系装置に送信する機能を有し、
前記送信系装置は、前記受信系装置に、前記メタデータ送信装置から受信した前記制作者情報と前記コンテンツ送信装置から受信した前記識別子との突き合わせで、前記制作されたメタデータから前記コンテンツに対するアクセスの可否を制御可能とさせたことを特徴とする送信系装置が得られる。
【発明の効果】

【００１６】
本発明によれば、メタデータの制作者を示す制作者情報（署名値）とコンテンツを再生するのに必要なライセンス情報に埋め込まれた識別子（メタデータアクセス制御記述子）を突き合わせることにより、メタデータからコンテンツへのアクセス可否を判断することが出来る。
【発明を実施するための最良の形態】
【００１７】
以下に述べる本発明の実施例では、メタデータ中に埋め込まれる、該メタデータを制作した制作者を示す制作者情報が、その制作者の電子署名である場合を例に説明するが、制作者情報は、電子署名に限らず、メタデータを制作した制作者を示すその他の情報であっても良い。ここで、メタデータを制作した制作者とは、メタデータの中にメタデータのインスタンス（実体）自体を作成した作成者か、或いは、そのメタデータを追加編集した制作者かである。
【００１８】
具体的には、以下の実施例では、ARIB STD-B38で定義されたメタデータの中にメタデータのインスタンス（実体）自体を作成した作成者（或いはそのメタデータを追加編集した制作者）の電子署名（XML署名）を制作者情報として埋め込み、メタデータの作成者（或いは追加編集した制作者）を同定する。一方、コンテンツには、どのメタデータからのアクセスを許可するかを判断するための識別子を埋め込み、電子署名（XML署名）と識別子とを両者を突き合わせることで、制作されたメタデータからコンテンツに対するアクセスの可否を制御する。
【００１９】
以下、本発明の実施例について図面を参照して説明する。
【００２０】
図１を参照すると、本発明の第１の実施例によるアクセス制御システムが示されている。このアクセス制御システムは、メタデータからコンテンツへのアクセスを制御するためのものである。
【００２１】
このアクセス制御システムは、既に作成されたコンテンツ６Ａに対するメタデータ３Ａを作成するのに使用されるメタデータ作成機２を有する。すなわち、メタデータ作成機２を保持しているメタデータ制作者１が、既に作成されたコンテンツ６Ａに対するメタデータ３Ａをメタデータ作成機２上で作成する。
【００２２】
ここで、コンテンツ６Ａには、どのメタデータからコンテンツ６Ａへのアクセスを許可するかを示すメタデータアクセス制御記述子７Ａが埋め込まれている。典型的には、メタデータアクセス制御記述子７Ａは、コンテンツ６Ａへのアクセスが許可されるメタデータの制作者を示している。これは本発明の特徴の一つである。
【００２３】
図２を参照すると、メタデータ制作者１によって作成されたメタデータ（署名前メタデータ）が示されている。署名前メタデータにおいて、制作者の作成部１３の一つには、例えば、前述の野球中継番組のある打者のすべての打撃シーンの開始時間位置を示す情報が、メタデータのインスタンスとして、入れられる。
【００２４】
図１に戻って、メタデータ制作者１は、自身を証明する公開鍵証明書とそれに対応する秘密鍵を有している。メタデータ制作者１は、メタデータ３Ａの作成が終了すると、メタデータ作成機２上で、メタデータ３ＡにXML-Signatureで定義されるXML署名４Ａと署名に利用した公開鍵証明書５Ａを付加することで、作成者署名付きのメタデータを作成する。
【００２５】
図３を参照すると、上述の作成者署名付きのメタデータ３Ａが示されている。署名者の公開鍵証明書５Ａは、バイナリをBase64でエンコードした形でＸＭＬ形式の制作者１の署

名４Ａに埋め込まれる。

【００２６】

図１に戻って、コンテンツ６Ａは、放送用の通信手段である放送網１１を使って利用者に配布され、メタデータ３Ａは、ネットワーク（インターネット等の通信ネットワーク）１０を使って利用者に配布される。利用者は、ネットワーク１０に接続され、メタデータ作成機２から配布されたメタデータ３Ａをメタデータ３Ｂとして取得するメタデータ制御機８と、放送網１１からのコンテンツ６Ａをコンテンツ６Ｂとして取得するコンテンツ受信機９とを保持する。コンテンツ受信機９は、コンテンツ再生機能をも有するものである。利用者は、メタデータ制御機８を利用して、配送されてきたメタデータ３Ｂ（３Ａと同じ）にアクセスし、メタデータ３Ｂからコンテンツ６Ｂ（６Ａと同じ）へのアクセスが可能な場合には、メタデータ３Ｂに基づいたコンテンツ６Ｂのダイジェスト映像などを見ることが出来る。

【００２７】

上述では、コンテンツ６Ａを放送網１１、メタデータ３Ａをネットワーク１０を使って利用者に配布する方法を示したが、コンテンツ６Ａをネットワーク、メタデータ３Ａを放送網で配布してもよい。また、コンテンツ６Ａ及びメタデータ３Ａを両方とも放送網で配布してもよいし、コンテンツ６Ａ及びメタデータ３Ａを両方ともネットワークで配布してもよい。

【００２８】

この際、メタデータ制御機８が、メタデータ３Ｂからコンテンツ６Ｂにアクセスするときは、まず、メタデータ６Ｂに付与されているメタデータ制作者の署名４Ａを検証しメタデータ３Ｂが改竄されていないことを確認する。次に、メタデータ制作者の公開鍵証明書５Ａの中に記述されている公開鍵証明書の所有者の情報が格納されているサブジェクト(subject)領域の値を取得し、メタデータ３Ａの作成者を同定する。続いて、メタデータ制御機８は、コンテンツ受信機９にアクセスし、コンテンツ６Ｂのメタデータアクセス制御記述子７Ａを取得する。メタデータ制御機８は、メタデータアクセス制御記述子７Ａと公開鍵証明書の所有者の情報（RFC3280で規定される公開鍵証明書のsubject）を突き合わせることで、メタデータからコンテンツへのアクセス可能かどうか判断する。

【００２９】

すなわち、メタデータ制御機８は、公開鍵証明書の所有者の情報（RFC3280で規定される公開鍵証明書のsubject）がメタデータアクセス制御記述子７Ａにアクセスを許可するメタデータの制作者として記述されている場合には、メタデータ３Ｂからコンテンツ６Ｂへのアクセスを許可され、メタデータ３Ｂに基づいたコンテンツ６Ｂのダイジェスト映像などを見ることが出来る。

【００３０】

ここで、メタデータアクセス制御記述子７Ａに、あらゆるメタデータ制作者をアクセス許可するものとして記述しておいた場合には、どのメタデータ制作者でも、自分が作ったメタデータに基づいたコンテンツ６Ｂのダイジェスト映像などを自由に見ることが出来る。

【００３１】

また、メタデータ制御機８は、公開鍵証明書の所有者の情報（RFC3280で規定される公開鍵証明書のsubject）がメタデータアクセス制御記述子７Ａに記述されているメタデータの制作者として識別（或いは、特定）される場合でも、メタデータ３Ｂからコンテンツ６Ｂへのアクセスを許可され、メタデータ３Ｂに基づいたコンテンツ６Ｂのダイジェスト映像などを見ることが出来る。

【００３２】

なお、前記電子署名は、公開鍵基盤（ＰＫＩ）技術にもとづき前記制作者としての署名者を特定することができるものであれば良い。

【００３３】

図４を参照すると、本発明の第２の実施例によるアクセス制御システムが示されている

。このアクセス制御システムは、上述したコンテンツ６Ａ（図１）を作成するコンテンツ作成機２２と、メタデータ作成機２（図１）及びコンテンツ作成機２２とメタデータ制御機８（図１）及びコンテンツ受信機９（図１）との間に接続されたメタデータ制御機２９及びコンテンツ受信及び送信機３０とを、更に有する。図示の例では、メタデータ制御機２９及びコンテンツ受信及び送信機３０は、メタデータ作成機２及びコンテンツ作成機２２にネットワーク２５を介して接続されると共に、メタデータ制御機８及びコンテンツ受信機９にネットワーク１０及び放送網１１を介して接続される。

【００３４】

この場合、ネットワーク２５は、ネットワーク１０と同じネットワークが用いられても良い。或いは、メタデータ作成機２及びコンテンツ作成機２２とメタデータ制御機２９及びコンテンツ受信及び送信機３０との接続に、ネットワーク２５を用いる代りに、ネットワーク１０及び放送網１１を用いても良い。

【００３５】

このアクセス制御システムにおいて、コンテンツ受信及び送信機３０は、ネットワーク２５からのコンテンツ６Ａをコンテンツ６Ａ'として取得する図１のコンテンツ受信機９（コンテンツ再生機能をも有する）の機能と、コンテンツ６Ａ'を放送網１１を介して送信する送信機の機能とを有する。コンテンツ受信及び送信機３０に続いて、コンテンツ受信機９は、放送網１１からのコンテンツ６Ａ'をコンテンツ６Ｂとして取得する。

【００３６】

メタデータ制御機２９は、ネットワーク２５からのメタデータ３Ａをメタデータ３Ａ'として取得する。メタデータ制御機２９は、ネットワーク２５からのメタデータ３Ａをメタデータ３Ａ'として取得する。メタデータ制御機２９は、図１で述べたメタデータ制御機８と同様に、メタデータ制作者１がコンテンツ６Ａ'内のメタデータアクセス制御記述子７Ａにアクセスを許可するメタデータの制作者として記述されているか、識別（或いは、特定）される場合には、メタデータ３Ａ'からコンテンツ６Ａ'へのアクセスを許可される。メタデータ制御機２９及びコンテンツ受信及び送信機３０の利用者（メタデータ制作者３４）は、メタデータ３Ａ'に基づいたコンテンツ６Ａ'のダイジェスト映像などを見ることが出来る。

【００３７】

メタデータ制御機２９は、メタデータ３Ａ'をネットワーク１０を介して送信する機能をも有する。メタデータ制御機２９に続いて、メタデータ制御機８は、ネットワーク１０からのメタデータ３Ａ'をメタデータ３Ｂとして取得する。メタデータ制御機８及びコンテンツ受信機９の利用者も、図１で述べたとおり、メタデータ制作者１がコンテンツ６Ｂ内のメタデータアクセス制御記述子７Ａにアクセスを許可するメタデータの制作者として記述されているか、識別（或いは、特定）される場合には、メタデータ３Ｂからコンテンツ６Ｂへのアクセスを許可され、メタデータ３Ｂに基づいたコンテンツ６Ｂのダイジェスト映像などを見ることが出来る。

【００３８】

このアクセス制御システムにおいて、メタデータ作成機２でメタデータ制作者１がコンテンツ６Ａに対するメタデータ３Ａを作成し、メタデータ制御機２９でメタデータ制作者３４がメタデータ３Ａに追加編集を加えて、メタデータ３Ａ'としたとする。

【００３９】

図５を参照すると、メタデータ制御機２９でメタデータ制作者３４がメタデータ３Ａに追加編集を加えた場合の署名されたXML形式のメタデータ３Ａ'が示されている。この場合、署名されたXML形式のメタデータ３Ａ'内には、メタデータ制作者１とメタデータ制作者３４の二人が作成したメタデータがメタデータ制作者１の作成部１３（図２）とメタデータ制作者３４の作成部３７とが混在し、メタデータ制作者１及びメタデータ制作者３４のＸＭＬ署名がメタデータ制作者１の署名４Ａ（図２）及びメタデータ制作者３４の署名３９としてメタデータ３Ａ'に埋め込まれることになる。

【００４０】

図４において、しかしながら、署名３９内のＸＭＬ署名の公開鍵証明書の所有者（メタデータ制作者３４）がコンテンツ６Ａ’内のメタデータアクセス制御記述子７Ａにアクセスを許可するメタデータの制作者として記述されていないか、識別（或いは、特定）されない場合には、メタデータ制御機２９において、メタデータ３Ａ’からコンテンツ６Ａ’へのアクセスは許可されず、メタデータ３Ａ’に基づいたコンテンツ６Ａ’のダイジェスト映像などは見ることが出来ない。

【００４１】

このように、メタデータ作成者３４が、コンテンツ受信及び送信機３０において受信したコンテンツ６Ａ’にアクセスするメタデータを作成部３７としてメタデータ制御機２９において、追加したとしても、コンテンツ作成機２２でメタデータアクセス制御記述子７Ａを作成する段階で権限を与えられていなければ、そのメタデータを有効に機能させない、メタデータからコンテンツへのアクセス制御が、実現する。

【００４２】

ここで、図４において、受信系装置が、メタデータ制御機２９とコンテンツ受信及び送信機３０との組合せ、或いは、メタデータ制御機８とコンテンツ受信機９との組合せであるとする。更に、図４において、送信系装置が、コンテンツを前記受信系装置に送信するコンテンツ送信装置（コンテンツ作成機２２）と、前記コンテンツに対して制作されたメタデータを前記受信系装置に送信するメタデータ送信装置（メタデータ作成機２）とを有するものとする。

【００４３】

この場合、メタデータ送信装置（メタデータ作成機２）は、前記制作されたメタデータを、前記制作されたメタデータ中に該メタデータを制作した制作者の電子署名を埋め込んだ状態にて前記受信系装置に送信する機能を有し、コンテンツ送信装置（コンテンツ作成機２２）は、前記コンテンツを再生するのに必要なライセンス情報を、該ライセンス情報に、どのメタデータからコンテンツへのアクセスを許可するかを示す識別子を埋め込んだ状態にて前記受信系装置に送信する機能を有するものである。そして、前記送信系装置は、前記受信系装置に、前記メタデータ送信装置（メタデータ作成機２）から受信した前記電子署名と前記コンテンツ送信装置（コンテンツ作成機２２）から受信した前記識別子との突き合わせで、前記制作されたメタデータから前記コンテンツに対するアクセスの可否を制御可能とさせたものである。

【００４４】

次に、図４の実施例の各部分について詳細に説明する。

【００４５】

（メタデータ制作機２）

図６を参照すると、メタデータ作成機２は、ＩＣ(Integrated Circuit)カードリーダライタ４５が接続された、パーソナルコンピュータなどの情報処理装置である。メタデータ作成機２は、例えばソフトウエアで実現されるメタデータ作成部４１とメタデータ送信部４２とから構成される。メタデータ作成機４０は、コンテンツ６Ａ（図４）対応するメタデータ３Ａ（図４）を作成する機能、作成したメタデータ３Ａに対して電子署名を付与する機能を有し、電子署名に利用する公開鍵証明書、秘密鍵を格納したＩＣカード４６へアクセスための機能を有し、ＩＣカードリーダライター４５が接続される。

【００４６】

メタデータ作成部４１は、コンテンツ６Ａに対応するメタデータ３Ａを作成する機能を有し、作成したコンテンツ６Ａに対し、電子署名を付加する機能として署名生成部４３を有するソフトウエアで構成される。また、作成したメタデータ３Ａを使いコンテンツ６Ａを再生するためのコンテンツ再生制御部４４を有する。

【００４７】

メタデータ送信部４２は、メタデータ作成部４１で作成されたメタデータ３Ａをインターネット等の通信ネットワーク２５（図４）を介してメタデータ制御機２９（図４）へ転送する機能を有する。

【００４８】
署名生成部４３は、作成されたメタデータ３Ａに対して電子署名を付与する機能を有する。署名対象文書に対し、W3Cの規格であるXML-Signature形式の署名文書を作成し、署名のためのハッシュ値を生成、ＩＣカードリーダライター４５を介したＩＣカード４６により署名値を生成し、生成された署名値をXML署名文書に埋め込むことにより署名を実行する。また、ＩＣカード４６に格納されている署名者の公開鍵証明書を署名対象文書に埋め込む機能も有する。
【００４９】
ＩＣカード４６は、秘密鍵と公開鍵証明書が格納でき、内部で暗号計算を実行できる機能を有する。ＩＣカードリーダライター４５経由で、署名対象文書のハッシュ値が渡されると、それを暗号化することにより署名値を生成し、それをＩＣカードリーダライタ４５経由で署名生成部４３へ返却する。
【００５０】
ＩＣカードリーダライタ４５は、パーソナルコンピュータなどの情報処理装置からの命令によりＩＣカード４６内の情報を読み取る機能、およびＩＣカード４６にＩＣカード４６内に格納された鍵を用いた電子署名のための暗号計算の実行を命令する機能を有する。
【００５１】
コンテンツ再生制御部４４は、メタデータ３Ａの内容に従いコンテンツ作成機２２（図４）へコンテンツの部分再生を命令する機能を有する。
【００５２】
（メタデータ制御機２９（或いは８））
図７を、図４と併せ参照して、メタデータ制御機４７は、ＩＣカードリーダライタ５２が接続されたパーソナルコンピュータなどの情報処理装置である。メタデータ制御機４７は、ソフトウエアプログラムで実現される署名生成・検証機能部４９とコンテンツ再生制御部５０とを含むメタデータ編集部４８と、メタデータ送受信部５１とから構成される。
【００５３】
ICカードリーダライター５２及びＩＣカード５３は、メタデータ作成機４０に接続されているものと同等のものである。
【００５４】
メタデータ編集部４８は、メタデータ３Ａ’（或いは３Ｂ）を編集する機能と、編集した部分に対し、署名生成・検証機能部４９とＩＣカードリーダライタ５２とＩＣカード５３とを利用して、電子署名を付与する機能と、署名生成・検証機能部４９を使って、メタデータ３Ａ’（或いは３Ｂ）に付与された署名および証明書を検証する機能と、コンテンツ６Ａ’（或いは６Ｂ）の再生制御を行うコンテンツ再生制御部５０を有する。
【００５５】
署名生成・検証機能部４９は、メタデータ作成機２と同様の署名生成機能と、与えらえらたメタデータの署名値を検証する機能と、証明書の検証機能を有する。
【００５６】
コンテンツ再生制御部５０は、メタデータ３Ａ’（或いは３Ｂ）の内容に従いコンテンツ受信及び送信機３０（或いはコンテンツ受信機９）へコンテンツ６Ａ’（或いは６Ｂ）の部分再生を命令する機能を有する。また、コンテンツ再生制御部５０は、再生時にメタデータ３Ａ’（或いは３Ｂ）からコンテンツ６Ａ’（或いは６Ｂ）へアクセス可能かどうかを判断するために利用するメタデータアクセス制御記述子７Ａを、コンテンツ６Ａ’（或いは６Ｂ）から取得する機能を有する。また、コンテンツ再生制御部５０は、メタデータ３Ａ’（或いは３Ｂ）に埋め込まれているメタデータ作成書署名の中からメタデータ制作者の公開鍵証明書を取得し、公開鍵証明書の所有者から署名者を同定する機能を有する。同定した署名者と、取得したメタデータアクセス制御記述子７Ａを比較しコンテンツ６Ａ’（或いは６Ｂ）へのアクセス可否を判断する機能を有する。
【００５７】
（コンテンツ作成機２２内の送信機）

図８を、図４と併せ参照して、コンテンツ作成機２２内の送信機は、コンテンツを記憶しているコンテンツ記憶部５４、符号化部５５、スクランブル部５６をもつコンテンツ生成手段５７と、コンテンツ鍵Kc生成のためのコンテンツ鍵生成部５９、メタデータアクセス制御情報生成部６０、コンテンツを再生するのに必要なライセンス情報（Kc伝送用ECM(Entitlement Control Message)/EMM(Entitlement Management Control Message)）を生成するKc伝送用ECM/EMM生成部６１をもつ鍵生成手段５８と、コンテンツ生成手段５７で生成した暗号化コンテンツと、鍵生成手段５８で生成した鍵を多重化する多重化手段６３から構成される。

【００５８】

コンテンツ記憶部５４は、映像、音声またはデータをコンテンツ６Ａとして記憶するハードディスクなどの記憶装置で構成される。

【００５９】

符号化部５５は、映像、音声またはデータをMPEG(Motion Picture Experts Group)-2 TS(Transport Stream)に符号化する符号化装置で構成される。

【００６０】

コンテンツ鍵生成部５９は、共通鍵暗号化方式でコンテンツを暗号化するための暗号鍵(コンテンツ鍵Kc)をコンテンツ毎に生成し、コンテンツを識別するためのコンテンツ識別を割り当て、コンテンツ識別ごとにコンテンツ鍵を管理する。

【００６１】

スクランブル部５６は、符号化したコンテンツを、コンテンツ鍵生成部５９で生成したコンテンツ鍵で暗号化し、暗号化コンテンツを生成する。

【００６２】

メタデータアクセス制御情報生成部６０は、コンテンツ６Ａに対してメタデータ利用を許可するための、メタデータアクセス制御記述子７Ａを生成する。メタデータアクセス制御記述子７Ａは、メタデータ制作者自身の識別コードであるメタデータ制作者識別、メタデータ制作者の属性（コンテンツプロバイダー兼メタデータ制作者、専業メタデータ制作者、利用者（ユーザ）など）を示すメタデータ制作者種別から構成される。

【００６３】

Kc伝送用ECM/EMM生成部６１は、コンテンツ鍵Kc、メタデータアクセス制御情報（メタデータアクセス制御記述子７Ａ）、およびワーク鍵或いはマスター鍵６２を含んだ、ARIB-STDB25「デジタル放送におけるアクセス制御方式」で規定されるセクション形式のKc伝送用ECMまたはKc伝送用EMMを生成する。すなわち、Kc伝送用ECM/EMM生成部６１において、メタデータアクセス制御情報（メタデータアクセス制御記述子７Ａ）がコンテンツを再生するために必要となるライセンス情報Kc伝送用ECMまたはKc伝送用EMMに埋め込まれる。Kc伝送用ECMは、ワーク鍵６２で、Kc伝送用EMMはマスター鍵６２で暗号化する。マスター鍵６２は、受信機ごとに付与される共通鍵暗号化方式の暗号鍵である。ワーク鍵６２は、事業者ごとなどの単位で付与される共通鍵暗号化方式の暗号鍵であり、Kc伝送用ECMを受信させたい受信機に対して予め共有化される暗号鍵であり、おのおのの受信機をグループ化するための暗号鍵である。すなわち、Kcを予めワーク鍵を共有化した受信機に対して一斉配信したい場合は、Kc伝送用ECMを用い、各々の受信機に個別にKcを配信したい場合は、Kc伝送用EMMを用いる。

【００６４】

Kc伝送用ECM/EMM（ライセンス情報）を放送により送る場合、多重化手段６３の多重化部６４は、コンテンツ生成手段５７の暗号化コンテンツ、ワーク鍵で暗号化したKc伝送用ECM/EMMの多重化を行い変調し放送として送出する。

【００６５】

ここで、各々の受信機に個別にKcを配信する場合にはKc伝送用EMM（ライセンス情報）をTCP/IP(Transmission Control Protocol/Internet Protocol)を利用した通信ネットワークを用いて個別に配信する。

【００６６】

（コンテンツ受信及び送信機３０内の送信機）

コンテンツ受信及び送信機３０内の送信機も、図８に示したコンテンツ作成機２２内の送信機と同様の構成を有する。ただし、コンテンツ生成手段５７のコンテンツ記憶部５４には、コンテンツ受信及び送信機３０内の受信機にて受信したコンテンツ作成機２２からのコンテンツ（映像、音声またはデータ）を記憶するものである。

【００６７】

（コンテンツ受信機９）

図９を、図４と併せ参照して、コンテンツ受信機９は、デスクランブル部６７、復号化部６９をもつコンテンツ復号手段と、Kc伝送用ECM/EMM復号部７０、コンテンツ鍵記憶部７２、メタデータアクセス制御情報記憶部７３をもつセキュリティモジュール７４と、暗号化コンテンツ６６と鍵情報との分離を行う分離手段とから構成される。

【００６８】

セキュリティモジュール７４は、外部から不正に情報を取り出すことができない耐タンパーなモジュールであり、ＩＣカード等で構成される。このセキュリティモジュール７４は、第３者機関で厳重に発行、管理が行われる。

【００６９】

分離部６５は、受信した放送を復調し、MPEG-2 TSレベルで、暗号化コンテンツ６６と、Kc伝送用ECM/EMM７６を分離する。

【００７０】

Kc伝送用ECM/EMM復号化部７０は、受信したKc伝送用ECMをワーク鍵７１で、Kc伝送用EMMをマスター鍵７１で暗号復号し、コンテンツ鍵（Kc）６８及びメタデータアクセス制御情報（メタデータアクセス制御記述子７Ａ）７５を取り出しコンテンツ鍵記憶部７２及びメタデータアクセス制御情報記憶部７３に記憶する。このように、コンテンツ鍵（Kc）６８及びメタデータアクセス制御情報（メタデータアクセス制御記述子７Ａ）７５をセキュリティモジュール７４で安全に記憶する。

【００７１】

この際、コンテンツ鍵記憶部７２は、コンテンツ識別ごとにコンテンツ鍵６８を記憶する。

【００７２】

メタデータアクセス制御情報記憶部７３は、コンテンツ識別ごとにメタデータアクセス制御情報（メタデータアクセス制御記述子７Ａ）７５を記憶する。

【００７３】

デスクランブル部６７は、セキュリティモジュール７４から得られるコンテンツ鍵６８で、暗号化コンテンツを暗号復号する。

【００７４】

復号化部６９は、受信したMPEG-2 TSで符号化したコンテンツを復号し、コンテンツ６Ｂとしての映像・音声情報またはデジタルデータを取り出す。

【００７５】

（コンテンツ受信及び送信機３０の受信機）

コンテンツ受信及び送信機３０内の受信機も、図９に示したコンテンツ受信機と同様の構成を有し、コンテンツ作成機２２からのコンテンツ（映像、音声またはデータ）を、コンテンツ６Ａ'として受信する。

【００７６】

（その他）

図４において、ネットワーク２５、ネットワーク１０は、インターネット等の通信ネットワークでメタデータの伝送を行う。

【００７７】

放送網１１は、既存の放送網で映像再生機間でコンテンツの配信をおこなう。

【００７８】

次に、図４の実施例において、メタデータ制御機８及びコンテンツ受信機９の利用者も

、メタデータ追加を行った場合の動作を、以下に説明する。

【００７９】

図４において、コンテンツ自身はあらかじめ作成しておき、コンテンツ作成機２２に格納する。図４のコンテンツ作成機２２の詳細なブロック図が図８である。

【００８０】

図８において、コンテンツ６Ａ（図４）はコンテンツ記憶部５４で記憶される。コンテンツ作成機２２は、コンテンツを暗号化してコンテンツ受信機９（或いはコンテンツ送信及び受信機３０）に送信するため暗号化鍵（コンテンツ鍵Ｋｃ）をコンテンツごとに生成し、コンテンツを識別するためにコンテンツ識別を割り当て、コンテンツ識別毎にコンテンツ鍵を管理する。

【００８１】

コンテンツはコンテンツ記憶部５４より読み出され、符号化部５５でＭＰＥＧ－２ ＴＳ(Transport Stream)に符号化される。符号化されたコンテンツはコンテンツ鍵生成部５９で生成したコンテンツ鍵を使用してスクランブル部５６で暗号化され、暗号化コンテンツとして生成される。

【００８２】

メタデータからコンテンツへのアクセス制御を実現するためには、コンテンツにアクセス制御パラメータを埋め込む必要がある。そこで、メタデータアクセス制御情報生成部６０でアクセス制御パラメータとなるメタデータアクセス制御記述子７Ａを生成する。メタデータアクセス制御記述子７Ａは、メタデータ制作者自身の識別コードであるメタデータ制作者識別と、メタデータ制作者の属性（コンテンツプロバイダー兼メタデータ制作者、専業メタデータ制作者、利用者（ユーザ）など）を示すメタデータ制作者種別とから構成される。

【００８３】

メタデータ制作者種別を記述するメタデータアクセス制御記述子１のデータ構造は、図１０の上表のようになる。メタデータ制作者識別を記述するメタデータアクセス制御記述子２のメタデータ構造は、図１０の下表のようになる。

【００８４】

図８において、生成されたコンテンツ識別、コンテンツ鍵及びメタデータアクセス制御情報は、Kc伝送用ECM/EMM生成部６１でARIB STD-B25「デジタル放送におけるアクセス制御方式」で規定されるセクション形式のＫｃ伝送用ＥＣＭまたはＫｃ伝送用ＥＭＭとしてワーク鍵またはマスター鍵６２で暗号化される。マスター鍵６２は受信機毎に付与される共通鍵暗号化方式の暗号鍵であり、ワーク鍵６２は事業者毎などの単位で付与される共通鍵暗号化方式の暗号鍵である。

【００８５】

一方、図４のメタデータ制作者１は、メタデータ作成機２でコンテンツ６Ａに対するメタデータ３Ａを作成する。図６は、メタデータ作成機１の詳細なブロック図である。

【００８６】

図６において、メタデータ制作者１は、コンテンツ６Ａに対するメタデータ３Ａをメタデータ作成機２のメタデータ作成部４１で作成する。作成されるメタデータは、図２のようにARIB STD-B38に定義されているものに従ったＸＭＬ形式の文書となる。メタデータ制作者１は、図２のようなＸＭＬ形式のメタデータを作成した後、図３のように、作成したメタデータに対するメタデータ制作者署名４Ａ（XML-Signature に従う）を付与する。

【００８７】

図３において、このメタデータ制作者署名４Ａには制作者のメタデータ制作者公開鍵証明書５Ａを含めておく。署名後のメタデータは、署名されたＸＭＬ形式のメタデータ３Ａのようになる。署名対象が文書全体或いは制作者１の作成部１３とすると、XML署名文書は、XML-Signature Syntax and Processingに従った形式で制作者の署名４Ａとしてメタデータに埋め込まれる。また、署名者の公開鍵証明書は、署名者の公開鍵証明書５Ａのような形で、証明書のXML-Signatureの規格に従い、制作者の署名４Ａに埋め込まれる。

【００８８】
図４において、第一次制作者１が作成した、メタデータ３Ａおよびコンテンツ６Ａはネットワーク２５を利用してコンテンツプロバイダーである第二次制作者に転送される（ここではメタデータ制作者３４と表現する）。
【００８９】
第二次制作者３４は、第一次制作者１からメタデータを３Ａ'として受信すると、図５に示すように、メタデータ制作者３４の作成部３７をメタデータ３Ａ'に追加する。
【００９０】
図５において、追加した後にメタデータ制作者３４が作成した部分のみに対する署名処理を施し、メタデータ制作者３４の署名３９としてメタデータに付与する。このメタデータ制作者３４の署名３９には、第二次制作者３４の公開鍵証明書であるメタデータ制作者公開鍵証明書を含めておく。このように、メタデータ制作者３４の署名３９がメタデータに埋め込まれる。
【００９１】
図４において、コンテンツ６Ａ'（６Ａと同じ）及びメタデータ制作者３４が作成したメタデータ３Ａ'は、ネットワーク１０及び放送網１１を利用して、メタデータ３Ａ'は利用者の端末であるメタデータ制御機８へメタデータ３Ｂとして配信し、コンテンツ６Ａ'はコンテンツ受信機９へコンテンツ６Ｂとして配信される。利用者は、配信されたメタデータ３Ｂに付加されているメタデータ制作者１の署名であるメタデータ制作者の署名４Ａ、メタデータ制作者３４の署名であるメタデータ制作者の署名３９（図５）を検証し、メタデータ３Ｂが改竄されていないことを確認する。その後、利用者は、メタデータ３Ｂに、図５における作成部３７と同様に、自分でメタデータ追加を利用者の作成部に作成し、図５における署名３９と同様に、自分の署名を追加することができる。
【００９２】
この場合、利用者は、自分でメタデータ追加を施したメタデータ３Ｂを用いたコンテンツ６Ｂのダイジェスト版の再生を実行する。このとき、メタデータ３Ｂには、再生対象のコンテンツ６ＢのフラグメントがARIB STD-B38に従った<SegmentInformation…> … </SegmentInformation>というタグの中に記述されており、その情報に従ってコンテンツ６Ｂのダイジェストの再生をコンテンツ受信機９に命令する。再生時には、本発明の最も重要な特徴であるメタデータ３Ｂからコンテンツ６Ｂへのアクセス制御情報をチェックしてから再生する。メタデータ３Ｂからコンテンツ６Ｂへのアクセス可・不可は、次のような手順で判断される。
【００９３】
手順１．メタデータ３Ｂに含まれる第１の署名（メタデータ制作者１の署名４Ａ）、第２の署名（メタデータ制作者３４の署名３９）、及び第３の署名（メタデータ制御機８及びコンテンツ受信機９の利用者の署名）を検証し、同時に署名の検証に必要な証明書も検証する。
【００９４】
手順２．メタデータ内の利用対象の部位を作成したのは誰かをその部分に対して付加されている署名から識別する。このとき、第１乃至第３の署名（ＸＭＬ署名形式の署名文書）の中にそれぞれ含まれているメタデータ制作者の公開鍵証明書の所有者から、所有者名および所有者の所属組織を特定する。公開鍵証明書の所有者属性はDN（Distinguished Name）とよばれる形式で表現され、cnの値は所有者名が登録され、ouの値を所有者所属組織が登録されている。また、cnの値は、図１０のメタデータアクセス制御識別と同じ命名規則が適用され、ouの値は、図１０のメタデータアクセス制御種別と同じ命名規則が適用される。
【００９５】
手順３．一方、コンテンツ受信機（再生機）９には、コンテンツ作成時にコンテンツ作成機２２のメタデータアクセス制御情報生成部６０（図８）で作成された、図１０の２つの表に従ったアクセス制御情報が、メタデータアクセス制御識別子７Ａとしてコンテンツ

６Ａと一緒に配信される。そこで、コンテンツ受信機（再生機）９にメタデータ制御機８から問い合わせてメタデータアクセス制御識別子７Ａの情報を取得する。

【００９６】

手順４．この際、図９のコンテンツ受信機（再生機）９は、メタデータ制御機８からの要求により、メタデータアクセス制御情報記憶部７３からメタデータアクセス制御情報７５（メタデータアクセス制御識別子７Ａ）を取り出し返却する。

【００９７】

手順５．コンテンツ受信機（再生機）９から返却されたメタデータアクセス制御記述子７Ａのメタデータアクセス制御識別及びメタデータアクセス制御種別と、利用対象となるメタデータを作成した３人の作成者の証明書の所有者属性のcn及びouとを付き合わせ、３人の作成者の証明書の所有者属性のcn及びouがメタデータアクセス制御記述子７Ａのメタデータアクセス制御識別及びメタデータアクセス制御種別と一致するか否かを判定することにより、アクセス制御を実現する。

【００９８】

３人の作成者の証明書の所有者の少なくとも一つが、メタデータアクセス制御記述子７Ａ中に記述されていれば、メタデータ３Ｂのうちのその所有者の作成した情報からはコンテンツ６Ｂへのアクセスが許可される。アクセスが許可された場合は、許可されたメタデータ３Ｂの情報に従ってコンテンツ受信機（再生機）９へコンテンツ６Ｂの部分再生やその他の情報の表示を命令する。コンテンツ受信機（再生機）９は指示に従いコンテンツ６Ｂを部分再生する。

【００９９】

以上説明したように、本発明の実施例は、別々に配信されるARIB STD-B38で定められた形式のメタデータ及びコンテンツにおいて、メタデータからコンテンツに対するアクセスの可否を、メタデータの署名者の公開鍵証明書の所有者の情報とコンテンツに埋め込まれたメタデータアクセス制御記述子を付き合わせることにより制御することを特徴とする。

【０１００】

本発明の実施例によれば、メタデータの作成者の署名値中の公開鍵証明書の所有者の情報とコンテンツに埋め込まれたメタデータアクセス制御記述子を付き合わせることにより、メタデータからコンテンツへのアクセス可否を判断することが出来る。

【０１０１】

更に、本発明の実施例によれば、証明書の所有者の情報に適切な階層構造をもたせ、その階層構造に対応したメタデータアクセス制御記述子（図１０のメタデータアクセス制御記述子１及び２）を定義することで、メタデータの作成者の組織属性に従ったメタデータからコンテンツへのアクセス制御を実現することが出来る。

【０１０２】

なお、上述した実施例の説明では、図８に示したように、コンテンツと、識別子（メタデータアクセス制御記述子）を含んだライセンス情報(Kc伝送用ECM/EMM)とを多重化手段６３で多重化して、送信したが、コンテンツとライセンス情報は、かならずしも併せて送る必要はなく、たとえば、コンテンツのみを送信しておき、後で、識別子（メタデータアクセス制御記述子）を埋め込んだライセンス情報(Kc伝送用ECM/EMM)を送信するといった手段を取ることも可能である。

【図面の簡単な説明】

【０１０３】

【図１】本発明の第１の実施例によるアクセス制御システムのブロック図である。

【図２】図１のアクセス制御システムのメタデータ作成機において、メタデータ制作者１によって作成された署名前メタデータを示す図である。

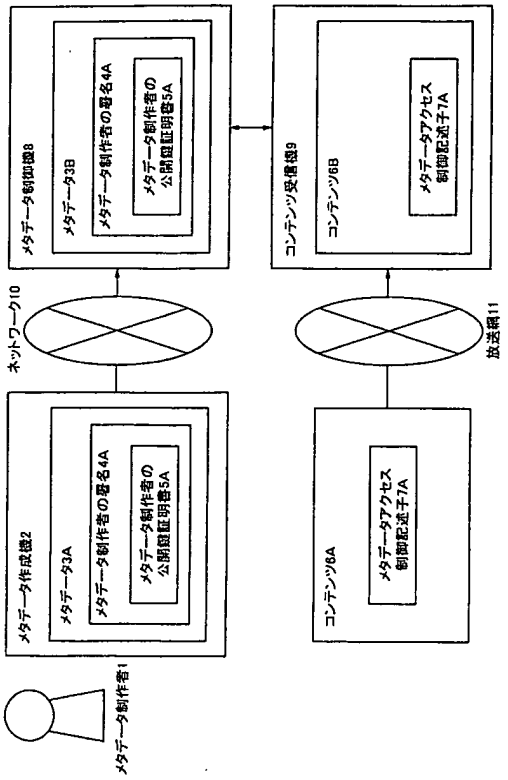
【図３】図１のアクセス制御システムのメタデータ作成機において、作成者付きのメタデータを示す図である。

【図４】本発明の第２の実施例によるアクセス制御システムのブロック図である。

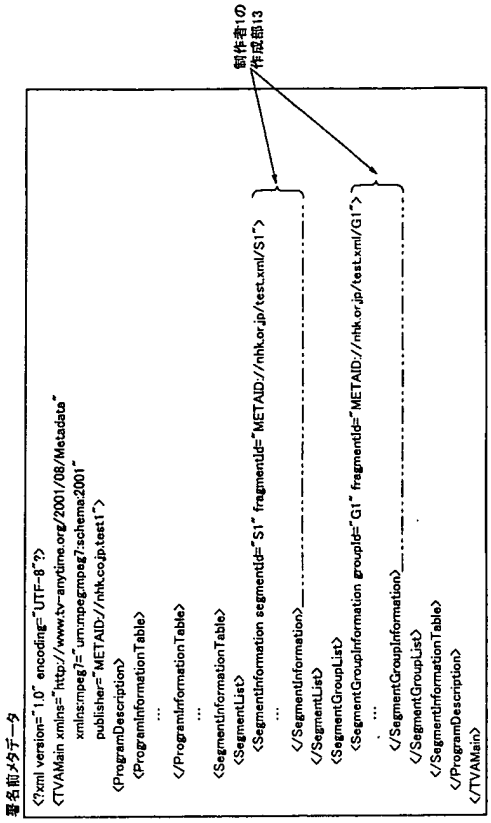
【図５】図４のアクセス制御システムのメタデータ制御機において、追加編集を加えた、

署名されたメタデータを示す図である。
【図６】図４のアクセス制御システムのメタデータ作成機のブロック図である。
【図７】図４のアクセス制御システムのメタデータ制御機のブロック図である。
【図８】図４のアクセス制御システムのコンテンツ作成機内の送信機のブロック図である。
【図９】図４のアクセス制御システムのコンテンツ受信機のブロック図である。
【図１０】図４のアクセス制御システムで用いられるメタデータアクセス制御記述子を説明するための図である。
【符号の説明】
【０１０４】
１　メタデータ制作者
２　メタデータ作成機
３Ａ　メタデータ
３Ａ'　メタデータ
４Ａ　XML署名
５Ａ　公開鍵証明書
６Ａ　コンテンツ
６Ａ'　コンテンツ
７Ａ　メタデータアクセス制御記述子
８　メタデータ制御機
９　コンテンツ受信機
１０　ネットワーク
１１　放送網
１３　制作者の作成部
２２　コンテンツ作成機
２５　ネットワーク
２９　メタデータ制御機
３０　コンテンツ受信及び送信機
３４　メタデータ制作者

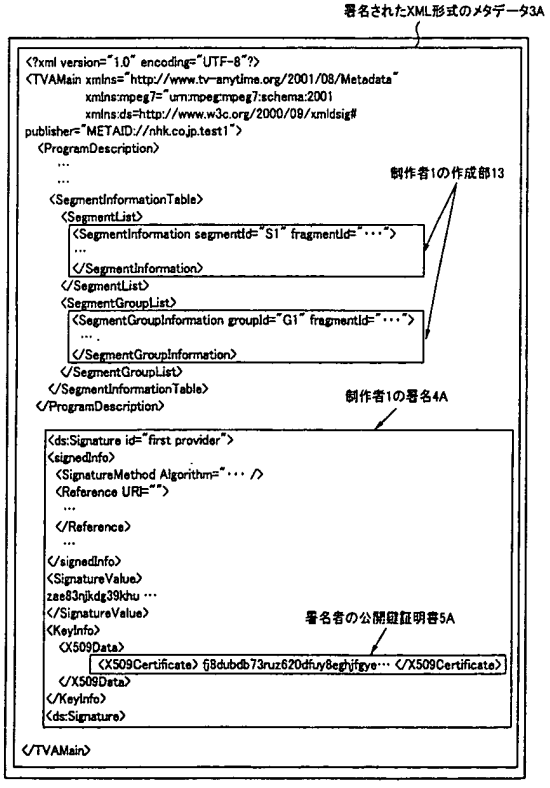
【図１】


メタデータ制御機8
メタデータ3B
メタデータ制作者の署名4A
メタデータ制作者の公開鍵証明書5A
コンテンツ受信機9
コンテンツ6B
メタデータアクセス制御記述子7A
ネットワーク10
放送網11
メタデータ作成機2
メタデータ3A
メタデータ制作者の署名4A
メタデータ制作者の公開鍵証明書5A
コンテンツ6A
メタデータアクセス制御記述子7A
メタデータ制作者1

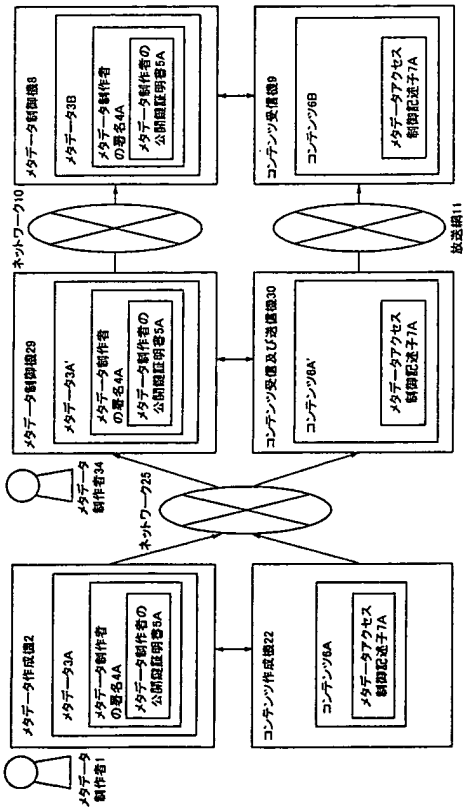
【図２】


署名前メタデータ
制作者1の作成部13
<?xml version="1.0" encoding="UTF-8"?>
<TVAMain xmlns="http://www.tv-anytime.org/2001/08/Metadata"
xmlns:mpeg7="urn:mpeg:mpeg7:schema:2001"
publisher="METAID://nhk.co.jp.test1">
<ProgramDescription>
<ProgramInformationTable>
...
</ProgramInformationTable>
...
<SegmentInformationTable>
<SegmentList>
<SegmentInformation segmentId="S1" fragmentId="METAID://nhk.or.jp/test.xml/S1">
...
</SegmentInformation>
</SegmentList>
<SegmentGroupList>
<SegmentGroupInformation groupId="G1" fragmentId="METAID://nhk.or.jp/test.xml/G1">
...
</SegmentGroupInformation>
</SegmentGroupList>
</SegmentInformationTable>
</ProgramDescription>
</TVAMain>

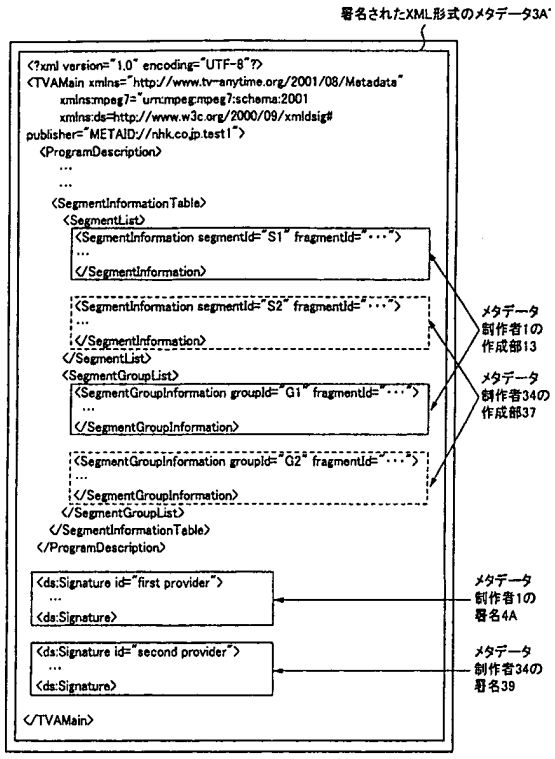
【図３】


署名されたXML形式のメタデータ3A
<?xml version="1.0" encoding="UTF-8"?>
<TVAMain xmlns="http://www.tv-anytime.org/2001/08/Metadata"
xmlns:mpeg7="urn:mpeg:mpeg7:schema:2001
xmlns:ds=http://www.w3c.org/2000/09/xmldsig#
publisher="METAID://nhk.co.jp.test1">
<ProgramDescription>
...
...
制作者1の作成部13
<SegmentInformationTable>
<SegmentList>
<SegmentInformation segmentId="S1" fragmentId="・・・">
...
</SegmentInformation>
</SegmentList>
<SegmentGroupList>
<SegmentGroupInformation groupId="G1" fragmentId="・・・">
...
</SegmentGroupInformation>
</SegmentGroupList>
</SegmentInformationTable>
</ProgramDescription>
制作者1の署名4A
<ds:Signature id="first provider">
<signedInfo>
<SignatureMethod Algorithm="・・・ />
<Reference URI="">
...
</Reference>
...
</signedInfo>
<SignatureValue>
zae83njkdg39khu ・・・
</SignatureValue>
<KeyInfo>
署名者の公開鍵証明書5A
<X509Data>
<X509Certificate> fj8dubdb73ruz620dfuy8eghjfgye・・・ </X509Certificate>
</X509Data>
</KeyInfo>
</ds:Signature>
</TVAMain>

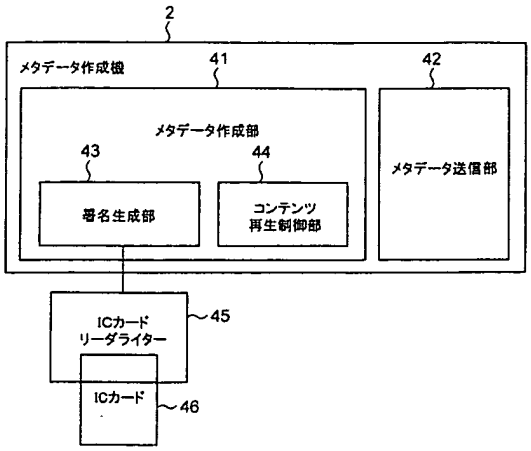
【図４】


メタデータ制御機8
メタデータ3B
メタデータ制作者の署名4A
メタデータ制作者の公開鍵証明書5A
コンテンツ受信機9
コンテンツ6B
メタデータアクセス制御記述子7A
ネットワーク10
放送網11
メタデータ制御機29
メタデータ3A'
メタデータ制作者の署名4A
メタデータ制作者の公開鍵証明書5A
コンテンツ受信及び送信機30
コンテンツ6A'
メタデータアクセス制御記述子7A
メタデータ制作者34
ネットワーク25
メタデータ作成機2
メタデータ3A
メタデータ制作者の署名4A
メタデータ制作者の公開鍵証明書5A
コンテンツ作成機22
コンテンツ6A
メタデータアクセス制御記述子7A
メタデータ制作者1

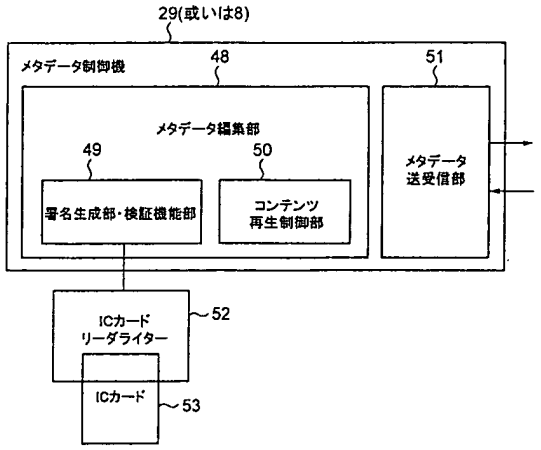
【図５】


署名されたXML形式のメタデータ3A'
<?xml version="1.0" encoding="UTF-8"?>
<TVAMain xmlns="http://www.tv-anytime.org/2001/08/Metadata"
xmlns:mpeg7="urn:mpeg:mpeg7:schema:2001
xmlns:ds=http://www.w3c.org/2000/09/xmldsig#
publisher="METAID://nhk.co.jp.test1">
<ProgramDescription>
<SegmentInformationTable>
<SegmentList>
<SegmentInformation segmentId="S1" fragmentId="・・・">
</SegmentInformation>
<SegmentInformation segmentId="S2" fragmentId="・・・">
</SegmentInformation>
</SegmentList>
<SegmentGroupList>
<SegmentGroupInformation groupId="G1" fragmentId="・・・">
</SegmentGroupInformation>
<SegmentGroupInformation groupId="G2" fragmentId="・・・">
</SegmentGroupInformation>
</SegmentGroupList>
</SegmentInformationTable>
</ProgramDescription>
<ds:Signature id="first provider">
<ds:Signature>
<ds:Signature id="second provider">
<ds:Signature>
</TVAMain>
メタデータ制作者1の作成部13
メタデータ制作者34の作成部37
メタデータ制作者1の署名4A
メタデータ制作者34の署名39

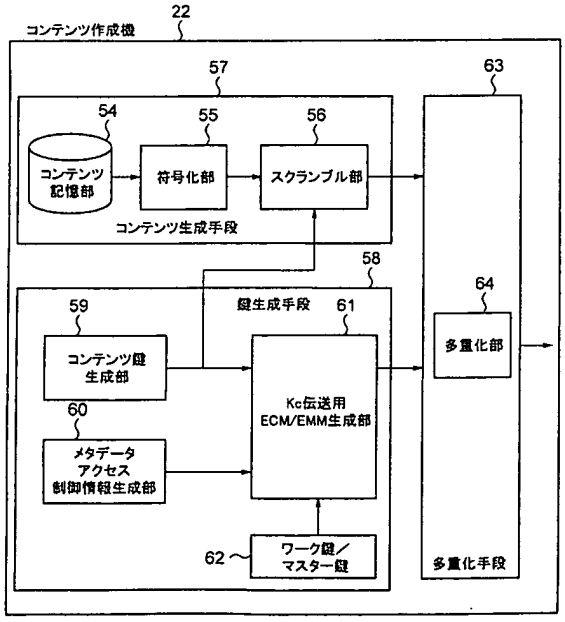
【図６】


2
メタデータ作成機
41
42
メタデータ作成部
43
44
署名生成部
コンテンツ再生制御部
メタデータ送信部
ICカードリーダライター
45
ICカード
46

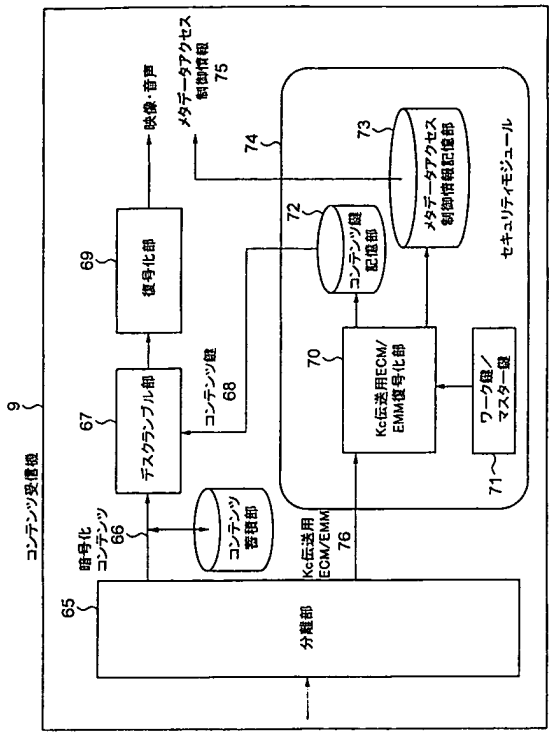
【図７】


29(或いは8)
メタデータ制御機
48
51
メタデータ編集部
49
50
署名生成部・検証機能部
コンテンツ再生制御部
メタデータ送受信部
ICカードリーダライター
52
ICカード
53

【図８】


22
コンテンツ作成機
57
63
54
55
56
コンテンツ記憶部
符号化部
スクランブル部
コンテンツ生成手段
58
64
59
鍵生成手段
61
コンテンツ鍵生成部
多重化部
60
Kc伝送用ECM/EMM生成部
メタデータアクセス制御情報生成部
62
ワーク鍵／マスター鍵
多重化手段

【図９】



【図１０】

記述子名	項目名	バイト長	備考
メタデータアクセス制御記述子1	記述子タグ	1	
	記述子長	1	メタデータ制作者識別をN個列挙した場合、値はN×10となる
	メタデータ制作者識別	10	最大10個まで列挙する

記述子名	項目名	バイト長	備考
メタデータアクセス制御記述子2	記述子タグ	1	
	記述子長	1	メタデータ制作者識別をN個列挙した場合、値はN×10となる
	メタデータ制作者識別	10	最大10個まで列挙する

フロントページの続き

(72)発明者 馬場 秋継
東京都世田谷区砧一丁目１０番１１号 日本放送協会放送技術研究所内
(72)発明者 中村 晴幸
東京都世田谷区砧一丁目１０番１１号 日本放送協会放送技術研究所内
(72)発明者 石川 清彦
東京都世田谷区砧一丁目１０番１１号 日本放送協会放送技術研究所内
(72)発明者 栗岡 辰弥
東京都渋谷区神南二丁目２番１号 日本放送協会放送センター内

Fターム(参考) 5B017 AA07 BA06 BA07 CA15
5J104 AA07 AA09 KA01 KA04 LA03 LA06 NA02 NA27 NA38 PA14